
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

CONTINGENCY PLANNING GUIDELINES FOR TABLE-TOP EXERCISE

Introduction

A tabletop exercise is a focused practice activity that places the participants in a simulated situation requiring them to function in the capacity that would be expected of them in a real event. Its purpose is to promote preparedness by testing policies and plans and by training personnel.

The exercise is a written scenario containing a set of circumstances and facts that create the need for the participants in the exercise to problem solve and make decisions that will bring the event to a conclusion with as few negative consequences as possible. By practicing and training with problem-solving tabletop exercises, it is possible for staff members to be able to establish a knowledge base that may help them to be able to develop the automatic responses which they will need when analytical thinking skills are compromised during an actual event.

The Disaster Recovery Institute International (DRII) defines a tabletop exercise as, “one method of exercising teams in which participants review and discuss the actions they would take per their plans, but do not perform any of these actions. The exercise can be conducted with a single team, or multiple teams, typically under the guidance of exercise facilitators.”

Planning the Exercise

No matter what type of exercise is being presented, it's best to have an exercise planning coordinator assigned. This person selects the type of exercise to be performed and is responsible for selecting the components of the plan to be exercised. For a tabletop exercise, it's the responsibility of the coordinator to:

- Identify the objectives;
- Develop an initial exercise scenario and narrative;
- Identify the participants;
- Chair the exercise participants meetings;
- Distribute minutes;

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

- Facilitate the exercise;
- Perform a post exercise analysis;
- Develop a scoring method relative to the response of the participants as their plans are implemented during the exercise.

Exercise Facilitator

The Exercise Facilitator may be a Business Continuity Plan Subject Matter Expert, or other individual identified by management. The primary role of the facilitator is to ensure that the tabletop exercise proceeds on schedule and achieves the desired result of determining the viability of the Business Continuity Plans. To achieve that result, there are several questions that can be asked as the exercise begins and through the discussion of issues and assignment of responsibility for corrective actions. The facilitator also has the option to introduce "roadblocks", such as unavailability of a key person or resource, to identify gaps or weaknesses in the documented business continuity strategies and plans. The facilitator may also add additional failure conditions during the exercise.

The Exercise Facilitator's responsibilities include:

- Keeping the session flowing (see Facilitator Leading Questions below);
- Introducing roadblocks during the exercise;
- Ensuring issues are documented;
- Keeping the session on schedule;
- Providing summary comments at the conclusion;
- Discussing next step activities and time frames.

The Scenario

The key to the tabletop exercise is the scenario. It must be definitive and sensible; a scenario related to threats that could occur and one that matches the organization's need at the time of the exercise.

The scenario should identify and describe the type of disaster that has occurred and the extent of damage or disruption to the facility and area. In addition, the scenario should detail what recovery capabilities are available and the status of backup or recovery resources. Finally, it should outline the time of the event and duration of the exercise.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

During the exercise, the scenario should enable the recovery teams to test the notification procedures (call trees and contact lists), recovery management, recovery operating procedures (tasks and responsibilities), the staffing of the teams and overall communications. Consideration must also be given to limitations as to what can be done in the exercise. It's best to identify any assumptions that need to be in place for the exercise.

A chronological sequence of events will illustrate the mock disaster by identifying:

- The hypothetical moment of the disaster (time of day, day of month, part of year);
- The cause of the disaster;
- The method of notification;
- A description of the events of the disaster leading to the declaration and activation of the plan;
- A description of the regional implications;
- A description of the role of the civil authorities and their activities during and after the disaster;
- Any actions that have been taken prior to activation of the plan;
- The damage to the facility;
- The status of all personnel;
- The status of alternate processing locations, vendors and suppliers, backup storage arrangements and utilities.

Based upon the effectiveness of the pre-exercise meetings, the exercise will almost run by itself with team members knowing what has to be accomplished. Exercising is a primary means of training. In any actual recovery effort, the best team members are usually those who have participated in exercises.

Post-Exercise Analysis

As soon as possible after the exercise, all participants should meet to discuss, evaluate, and document the exercise results. Topics would include a review of the exercise schedule (i.e., date, time, location), exercise objectives both logistically and operationally and the identification of personnel who supported exercise activities.

The planning team should then formulate recommendations based on the events that occurred during the exercise and start planning for next exercise.

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

**IT Contingency Planning: *IT Disaster Recovery
Planning***

Table-top Exercise Information Sources:

<http://www.coned.iup.edu/SafetyScience/Disaster/continuity.htm>

<http://www.epa.gov/safewater/watersecurity/tools/trainingcd/Pages/scenario8-s.html>

<http://www.recoverychronicles.com/MediaPR/eNewsletter/July2005/442/Article.asp>

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

CONTINGENCY PLANNING TABLE-TOP EXERCISE

Purpose

The Table-Top Exercise is intended to assist management and support staff in defining contingency business processes in order to ensure continuity of mission critical student and financial services in the event of a catastrophic loss of WAN connectivity for an extended period of time. It is essentially a sit-down, hands-on planning exercise for key personnel to run through the actions and procedures that need to be taken and the tools needed to maintain operations. Through the exercise, the issues or problems faced by college staff should be surfaced, run through on paper and in discussion, assessed and finally addressed with solutions drawn up to ensure that all efforts toward preparation and readiness for coping with a connectivity failure will be well coordinated and workable.

Exercise Scenario

Emergency Procedures, Planning Scenario 3: Loss of telecommunications (PSTN phone service). Under this scenario, the campus voice gateway router is not functioning.

On January 5, 2009 at 8:00 AM the John H. Daniel Campus of SVCC in Keysville, VA loses PSTN connectivity. The outage is discovered by the Daniel IT Staff and the problem is investigated. At approximately 9:00 AM the cause of the phone outage is determined to be due to the catastrophic failure of the campus voice gateway router. At that time the Daniel IT Network Administrator informs the provost (face-to-face meeting) of the problem and estimates time of problem resolution to be approximately 1:00 PM January 6th.

Implications: Loss of PSTN connectivity means that any business processes which depend on phone access to the outside world will not be available. For example local and long distance phone calls or faxes cannot be placed or received, native IP Telephony between campuses and VCCS sites will not be affected.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Assumptions:

- Replacement parts will be available within the acceptable downtime.
- One of the sites will survive the disaster.

- Backup media and documentation will be secure at the surviving site.

- Personnel can be made available to implement the Disaster Recovery Plan.

- In the event of total or partial loss of the College's computer services personnel, assistance will be available from the Virginia Community College System (VCCS) personnel to implement the Disaster Recovery Plan.

- In case of widespread regional disruption, access to emergency resources and personnel may be severely limited.

Objectives

The following objectives should be accomplished during the run through of this scenario:

- Identify the key personnel needed to respond to the contingency.
DRP Teams: Emergency Management, Technical Support (SVCC Security Plan, Attachment C 2.3. Also Section C, Plan Testing)

- Review the COOP and DRP as to provisions for continuity of operations.
(Sections C 1 and C 2 respectively, SVCC Security Plan)

- Review the *DRP and COOP Plan Testing* document. (Attachment C 2.1 SVCC Security Plan. Also Section B, Plan Testing)

- Define business processes for critical services as well as technical and procedural problems and their solutions. (Attachment C 1.1 *Recovery Strategies*, and *Manual Procedures* documents SVCC Security Plan. Also Sections E and F, Plan Testing)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

- Define the requirements and procedures for communication with other campuses. (Section C 2, SVCC Security Plan, *Emergency Procedures* document. Also Section D, Plan Testing)
- Identify issues for future table-top exercises. (To be included in the post exercise report as indicated below)

Exercise Procedure

All exercise participants will assemble in a suitable conference room. A computer with a connection to the college local area network is required. An LCD projector is highly recommended. The college ISO will be the facilitator for the Table-Top Exercise. The exercise facilitator should brief the exercise participants on the exercise scenario and moderate the discussion to ensure all objectives are accomplished. A current copy of the SVCC Security Plan will be used for the exercise. The following minimum exercise participants are recommended:

Selected members of the Emergency Management Team: (Attachment C 2.3)

- IT Disaster Planning Coordinator
- Network Administrator
- Information Security Officer
- College Provost
- Buildings and Grounds Supervisor
- Administrative, Financial, and Facilities Management Vice President

Selected members of the Technical Support Team: (Attachment C 2.3)

- Blackboard Administrator
- PeopleSoft Administrator
- Any other personnel deemed necessary for this team

Test Procedures:

The following is an order of operations for the table-top test:

- Satisfy all requirements of the “objectives” section of this document give above.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

- Define a testing scenario.
- Define Emergency Procedures which address the scenario. (Section D, Plan Testing)
- Define Recovery Strategies which address the scenario. (Section E, Plan Testing)
- Define a Recovery Plan Test which addresses the scenario. (Section B, Plan Testing)
- Identify a mission critical business process affected by the scenario. (Section E, Plan Testing)
- Apply applicable recovery strategies to the business process. (Sections E and F, Plan Testing)
- Document all results on the proper forms. (Section C, Plan Testing)

Post Exercise Reports

Immediately after conclusion of the exercise, a written post exercise report should be prepared to document the observations and findings of the exercise, identify recommendations for contingency management procedures, and to provide lessons learned on the conduct of the table-top exercise. The post exercise report on Continuity of Operations will be maintained by the college Information Security Officer.